



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/059,182	01/31/2002	Janne Suuronen	004770.00521	5357
22907	7590	09/07/2007		
BANNER & WITCOFF, LTD. 1100 13th STREET, N.W. SUITE 1200 WASHINGTON, DC 20005-4051			EXAMINER SHAW, YIN CHEN	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 09/07/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

---

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**MAILED**

**SEP 07 2007**

**Technology Center 2100**

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 10/059,182  
Filing Date: January 31, 2002  
Appellant(s): SUURONEN ET AL.

Christopher R. Glembocki  
Reg. No. 38,800

For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 06/04/2007 appealing from the Office action  
mailed 01/25/2006.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments**

The appellant's statement of the status of amendments contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

Fink et al. (U.S. Patent 6,496,935, Date of Patent: 12/2002)

Franczek et al. (U.S. Patent 6,397,335, Date of Patent: 05/2002)

Lyle (U.S. Patent 6,886,102, Date of Patent: 04/2005)

Radatti (U.S. Patent 6,721,424, Date of Patent: 04/2004)

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

**Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1, 3, 20-21, 32, 41-45 47, 49-51, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935).

- i. Referring to Claim 1:

As per Claim 1, Fink et al. disclose in a communication system including at least a first network [i.e., **external network 14 (Fig. 1)**] coupled to a destination [i.e., **protected nodes 20 in protected network 12 (Fig. 1)**] to which transmissions of data packets are made from the first network to the destination, a system for providing virus protection comprising:

a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and receives the data packets after reception by the firewall, tests the data packets, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus [i.e., **Therefore, according to the present invention, gateway 16 also features a pre-filtering module 30 which receives the packets before firewall 18, but which is preferably directly connected to protected network 12. Pre-filtering module 30 also preferably receives instructions from firewall 18, concerning packets which are permitted to enter protected network 12. These instructions are more preferably determined by firewall 18 from an analysis of one or more previously received and related packets, such that if a previously received and related packet has been permitted to enter protected network 12, then the current packet should also be permitted to enter protected network 12. Firewall 18 inspects the contents of such packet or packets, and base upon the**

**output of analysis module 24 with rulebase 26, determines whether packets from the corresponding connection should be permitted to enter and/or leave protected network 12 (line 67, Col. 6 and lines 1-4, Col. 7). Alternatively, if the packet is not permitted according to rule base 26, then the packet is optionally dropped (lines 55-56, Col. 5)];**

the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing and forwards the data packets of the second type for testing thereof **[i.e., Thus, if pre-filtering module 30 determines that the current packet is permitted to enter, then preferably pre-filtering module 30 passes the packet directly through to protected network 12 (lines 17-32, Col. 6). Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determined that the packet represents a violation which should be further inspected by firewall for validity (lines 39-42, Col. 7)].**

Fink et al. do not expressly disclose the virus scanning engine, coupled to the firewall, and the action of testing and disregarding of packet is associated to the virus. However, Fink et al. disclose the invention is implemented for the purpose of anti-spoofing and any packet(s) that cause violation **[i.e., Alternatively and optionally, even if only the**

**interface is not correct, pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 39-47, Col. 7 and Fig. 1); *where the pre-filtering module is coupled the firewall*].** Therefore, It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. to have the inspection and filtering of the packet on the virus explicitly since one would have been motivated to **provide security by controlling the traffic being passed, thus preventing illegal communication attempts, both within single networks and between connected networks (lines 31-33, Col. 1 in Fink et al.).** Thus, it would have been obvious to modify Fink et al. to obtain the invention as specified in claim 1.

ii. Referring to Claim 3:

As per Claim 3, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. wherein: the virus scanning engine tests the data packets of the second type and forwards those data packet which are tested to not contain a virus to the destination [i.e., **Alternatively and optionally, even if only the interface is not correct, pre-filtering**

module 30 may determined that the packet represents a violation which should be further inspected by firewall for validity (lines 39-42, Col. 7). Gateway 16 operates a firewall 18 for performing packet analysis and packet filtering (lines 33-34, Col. 5). Firewall 18 features a packet filter 22 for performing packet filtration. Packet filter 22 in turn is preferably composed of an analysis module 24 for analyzing packets and a rule base 26 (lines 42-46, Col. 5). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such tat the packet is permitted according to rule base 26, the packet filter 22 permits packet to enter protected network 12 (lines 48-53, Col. 5)].

iii. Referring to Claim 20:

As per Claim 20, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose the firewall drops any received data packet which are tested to be illegal according to firewall rules [i.e., Rule base 26 preferably contains one or more rules which are defined according to the preferences of the system administrator or other controller user (lines 46-48, Col. 5). Alternatively, if the packet is not permitted according to rule base 26, then the packet is optionally dropped (lines 55-56, Col. 5)].

iv. Referring to Claim 21:



As per Claim 21, the rejection of Claim 3 is incorporated. In addition, Claim 21 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

v. Referring to Claim 32:

As per Claim 32, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets [i.e., **Pre-filtering module 30 also preferably features a classification engine 38, including a data processor, for at least partially analyzing the information from the packet and for retrieving information from connection database 32 (lines 4-7, Col. 8). With the help of information and instructions retrieved from database 32 in memory 36, classification engine 38 then analyzes at least a portion of the information in each packet (lines 38-41, Col. 8);**

A virus detection data base, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine [i.e., **Packet filter 22 in turn is preferably composed of an analysis module for analyzing packets and a rule base 26. Rule base 26 preferably contains one or more rules which are defined according to the preferences of the**

**system administrator or other controlling user. Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in the rule base 26 (line 44-50, Col. 5)].**

vi. Referring to Claim 41:

As per Claim 41, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the destination is a local area network [i.e., **protected network 12 (Fig. 1)]**.

vii. Referring to Claim 42:

As per Claim 42, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the destination is a personal computer [i.e., **protected node 12 within the protected network 20 (Fig. 1)**]. Hereinafter, the term “network” includes a connection between any two or more computational devices which permits the transmission of data. Hereinafter, the term “computational” device” includes, but not limited to, personal computers (PC) having an operating system (lines 39-44, Col. 3)]

viii. Referring to Claim 43:

As per Claim 44, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the destination is a second network [i.e., **protected network 12 (Fig. 1)]**.

ix. Referring to Claim 44:

As per Claim 44, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the first network is a wide area network [i.e., **External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5)]**].

x. Referring to Claim 45:

As per Claim 45, the rejection of Claim 44 is incorporated. In addition, Fink et al. disclose the wide area network is the Internet [i.e., **External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5)]**].

xi. Referring to Claim 47:

As per Claim 47, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose the virus scanning engine decodes the data packets during determination if the data packets contain a virus [i.e., **Gateway 15 operates a firewall 18 for performing packet analysis and packet filtering (lines 33-34, Col. 5). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in the rule base 26 (lines 48-50, Col. 5). In addition, from the rules which are stored in rule base 26, analysis module 24 is able to determine one or more actions which should be associated with each connection. Examples of such actions include, but are not limited to, performing an accounting action in order to count the amount of data in the packet, encrypting/decrypting the packet,**

**performing network address translation (NAT) by rewriting the address fields, and so forth (lines 4-11, Col. 7)].**

xii. Referring to Claim 49:

As per Claim 49, it is a method claim corresponding to the system claim 1. Therefore, it is rejected with the same rationale applied against Claim 1 above.

xiii. Referring to Claim 50:

As per Claim 50, Fink et al. disclose in a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall and the virus scanning engine, coupled to the firewall, said firewall receiving the data packets, the virus scanning engine receiving the data packets after reception by the firewall, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus, said firewall classifying the received data packets into packets of a first type that cannot contain a virus and a second type that can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof, as in Claim 1. In addition, Fink et al. disclose a computer

program stored on a storage medium [i.e., **The device comprising: (a) a memory for storing at least one instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)] and the computer program when executed causing the virus scanning engine to execute at least one step of testing the data packets for the presence of a virus [i.e., **The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rules base 26 (lines 48-50, Col. 5)].****

xiv. Referring to Claim 51:

As per Claim 51, Fink et al. disclose a computer program in accordance with claim 50. In addition, Fink et al. disclose the computer program when executed causes the virus scanning engine to test the data packets of the second type and causes the virus scanning engine to forward those data packets which are tested to not contain a virus to the destination [i.e., **The method of the present invention could be described as a series of steps performed by a data processor, and**

as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12. Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12 (lines 48-53)].

xv. Referring to Claim 55:

As per Claim 55, the rejection of 50 is incorporated. In addition, Claim 55 encompasses limitations that are similar to those of Claims 20 and 32. Therefore, it is rejected with the same rationale applied against Claims 20 and 32. In addition, Fink et al. disclose the computer program [i.e., The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3); *where the computer software is executed by the processor to perform and control the functions*].

2. Claims 4-5, 11-12, 46, 48, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) as applied to claims 1, 3, and 47 above, and further in view of Franczek et al. (U.S. Patent 6,397,335).

i. Referring to Claim 4:

As per Claim 4, Fink et al. disclose a system in accordance with Claim 1. Fink et al. do not expressly disclose the data packets of the first type contain real time data. However, Franczek et al. disclose that stream data can be communicated between the client and server in the network environment **[i.e., Virus-free streams are reconstructed prior to communicating the data to the receiving party. In this way, the system is operative when there are multiple data streams defined between a client and a server (lines 20-24, Col. 12)]**. Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to have the stream data in the packet(s) communicating in the network environment since one would be motivated to **perform virus screening separately on each of a plurality of virtual channels included in an interactive session (lines 17-19, Col. 12 in Franczek**

et al.). Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 4.

ii. Referring to Claim 5:

As per Claim 5, the rejection of Claim 3 is incorporated. In addition, Claim 5 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale applied against Claim 4 above.

iii. Referring to Claim 11:

As per Claim 11, Fink et al. disclose a system in accordance with claim 1. Fink et al. do not expressly disclose the remaining limitation of the claim. However, Franczek et al. disclose a buffer **[i.e., a Preferably, each virus-screening processor has an associated memory device to store at least two packets (lines 13-14, Col. 5)]** which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus **[i.e., Alternatively the virus screening can be performed in-line by partitioning the file into small blocks of data, screening each block of data, and communicating each virus-free block data upon being screened (lines 64-67, Col. 11)]**. Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was



made to modify Fink et al. with Franczek et al. to have a storage buffer for a large packet(s) to be inspected since one would be motivated to **examine one more succeeding blocks since a virus signature could extend over several blocks of data (lines 3-5, Col. 12 in Franczek et al.)**. Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 11.

iv. Referring to Claim 12:

As per Claim 12, the rejection of Claim 3 is incorporated. In addition, Claim 12 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

v. Referring to Claim 46:

As per Claim 46, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose wherein: the first network is the Internet as in Claim 44 and the gateway is linked between the external network and destination. Fink et al. do not expressly disclose coupling to an Internet service provider and a modem coupled to the Internet service provider and one of local area or personal computer coupled to the modem. However, Franczek et al. disclose a personal computer linked to the internet service provider through the modem [**i.e., A user computer 400 having a modem 402 communicates with a modem 404 associated with an internet service providers 406 (lines 51-53,**

**Co. 12). Other connection means such as an integrated service digital network (ISDN), a digital subscriber line (DSL), or cellular data can be used to link the user computer 400 to the internet service provider 406 (lines 55-58, Col. 12)].** Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to integrate the gateway with the typical internet dial-up service setup in the network environment since one would be motivated to have **a service provider may subscribe to the virus screening service to protect its users from computer viruses by screening its transmitted computer data (lines 36-39, Col. 3 in Franczek et al.).** Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 46.

vi. Referring to Claim 48:

As per Claim 48, Fink et al. disclose a system in accordance with claim 47. Fink et al. does not expressly disclose that the virus scanning engine functions as a proxy for a destination processor which receives the data packets. However, Franczek et al. disclose the virus screening processors can function as a proxy server **[i.e., The herein-described virus-screening processors can provide or assist in providing a**

**proxy server or a functional equivalent of a proxy server (lines 3-5, Col. 5)].** Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to have the various components altogether within the gateway functioning as a proxy server in the network environment since one would be motivated to have **the virus-screening processor can create and communicate modified protocol-specific information such as a number of packets to be received, error detection and correction information, and packet serial numbers (lines 9-12, Col.5 in in Franczek et al.)**. Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 48.

vii. Referring to Claim 53:

As per Claim 53, the rejection of 51 is incorporated. In addition, Claim 53 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale applied against Claim 4.

3. Claims 13-14, 22-23, 27, 33, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 4-5 and 11-12 above.

i. Referring to Claim 13:

As per Claim 13, the rejection of Claim 4 is incorporated. In addition, Claim 13 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

ii. Referring to Claim 14:

As per Claim 14, the rejection of Claim 5 is incorporated. In addition, Claim 14 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

iii. Referring to Claim 22:

As per Claim 22, the rejection of Claim 4 is incorporated. In addition, Claim 22 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iv. Referring to Claim 23:

As per Claim 23, the rejection of Claim 5 is incorporated. In addition, Claim 23 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

v. Referring to Claim 27:

As per Claim 27, the rejection of Claim 12 is incorporated. In addition, Claim 27 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

vi. Referring to Claim 33:

As per Claim 33, the rejection of Claim 4 is incorporated. In addition, Claim 33 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

vii. Referring to Claim 36:

As per Claim 36, the rejection of Claim 11 is incorporated. In addition, Claim 36 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

4. Claims 28 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 13-14 above.

i. Referring to Claim 28:

As per Claim 28, the rejection of Claim 14 is incorporated. In addition, Claim 28 encompasses limitations that are similar to those of Claim 20.

Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 37:

As per Claim 37, the rejection of Claim 13 is incorporated. In addition, Claim 37 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

5. Claims 6-8 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) as applied to claims 1, 3, and 50 above, and further in view of Lyle (U.S. Patent 6,886,012).

i. Referring to Claim 6:

As per Claim 6, Fink et al. disclose a system in accordance with claim 1. Fink et al. do not expressly disclose wherein: the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which, in response to the alert, stops reception of a data stream containing the data packets. However, Lyle discloses that an alert message can be sent to various components in order to prevent them participating in flowing around the data containing malicious code [i.e., **In one embodiment, as described above, the responsive action for one or more types of incident may include sending an alert, such as by activating a pager and/or sending an e-mail message to alert**

**a network security administrator to the fact that an alert condition is present, or sending an appropriate message to a router or switch to stop a malicious flow of network traffic (lines 28-34, Col. 14)].**

Fink et al. and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to **share information about an attack, dynamically and without human intervention (lines 20-22, Col. 2).** Therefore, it would have been obvious to modify Fink et al. with Lyle to obtain the invention as specified in claim 6.

ii. Referring to Claim 7:

As per Claim 7, the rejection of Claim 1 is incorporated. In addition, Claim 7 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above.

iii. Referring to Claim 8:

As per Claim 8, the rejection of Claim 3 is incorporated. In addition, Claim 8 encompasses limitations that are similar to those of Claim 6.

Therefore, it is rejected with the same rationale applied against Claim 6 above.

iv. Referring to Claim 54:

As per Claim 54, the rejection of 50 is incorporated. In addition, Claim 54 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above. In addition, Fink et al. disclose the computer program [i.e., **The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3); where the computer software is executed by the processor to perform and control the functions**].

6. Claims 24-25 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Lyle (U.S. Patent 6,886,012) as applied to claims 6-7 above.

i. Referring to Claim 24:

As per Claim 24, the rejection of Claim 6 is incorporated. In addition, Claim 24 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 25:



As per Claim 25, the rejection of Claim 7 is incorporated. In addition, Claim 25 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iii. Referring to Claim 34:

As per Claim 34, the rejection of Claim 7 is incorporated. In addition, Claim 34 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

7. Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) as applied to claim 1 above, and further in view of Radatti (U.S. Patent 6,721,424).

i. Referring to Claim 40:

As per Claim 40, Fink et al. disclose a system in accordance with claim 1. Fink et al. do not expressly disclose wherein: the virus scanning engine, upon detection of a virus in the data packets, also alerts the destination that a virus has been detected. However, Radatti discloses an alert message is sent to notify the destination user of the virus presence in the data [i.e., **The gateway server 20 issues an appropriate alert or otherwise takes action to prevent transmission of the virus to the destination of the data transfer. For example, the**

**gateway server 20 may issue a message to the destination user station notifying the user that an incoming data transfer was determined to contain a virus (lines 30-36, Col. 4)].** Fink et al. and Radatti are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Radatti to have the alert message generated and sent to the destination upon detecting the malicious code since one would be motivated to **take action to prevent transmission of the virus to the destination of the data transfer (lines 31-32, Col. 4 in Radatti).** Therefore, it would have been obvious to modify Fink et al. with Radatti to obtain the invention as specified in claim 40.

8. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 4-5 above, and further in view of Lyle (U.S. Patent 6,886,012).

i. Referring to Claim 9:

As per Claim 9, Fink et al. and Franczek et al. disclose a system in accordance with claim 4. Fink et al. and Franczek et al. do not expressly disclose wherein: the virus scanning engine, when a virus is detected,

alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets. However, Lyle discloses that an alert message can be sent to various components in order to prevent them participating in flowing around the data containing malicious code [i.e., **In one embodiment, as described above, the responsive action for one or more types of incident may include sending an alert, such as by activating a pager and/or sending an e-mail message to alert a network security administrator to the fact that an alert condition is present, or sending an appropriate message to a router or switch to stop a malicious flow of network traffic (lines 28-34, Col. 14)**]. Fink et al., Franczek et al., and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Franczek et al. with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to **share information about an attack, dynamically and without human intervention (lines 20-22, Col. 2 in Lyle)**. Therefore, it would have been obvious to modify

Fink et al. and Franczek et al. with Lyle to obtain the invention as specified in claim 9.

ii. Referring to Claim 10:

As per Claim 10, the rejection of Claim 5 is incorporated. In addition, Claim 10 encompasses limitations that are similar to those of Claim 9. Therefore, it is rejected with the same rationale applied against Claim 9 above.

9. Claims 18-19, 26, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Franczek et al. (U.S. Patent 6,397,335), and Lyle (U.S. Patent 6,886,012) as applied to claims 9-10 above.

i. Referring to Claim 18:

As per Claim 18, the rejection of Claim 9 is incorporated. In addition, Claim 18 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

ii. Referring to Claim 19:

As per Claim 19, the rejection of Claim 10 is incorporated. In addition, Claim 19 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

iii. Referring to Claim 26:

As per Claim 26, the rejection of Claim 9 is incorporated. In addition, Claim 26 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iv. Referring to Claim 35:

As per Claim 35, the rejection of Claim 9 is incorporated. In addition, Claim 35 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

10. Claims 31 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Franczek et al. (U.S. Patent 6,397,335), and Lyle (U.S. Patent 6,886,012) as applied to claim 18 above.

i. Referring to Claim 31:

As per Claim 31, the rejection of Claim 18 is incorporated. In addition, Claim 31 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 39:

As per Claim 39, the rejection of Claim 18 is incorporated. In addition, Claim 39 encompasses limitations that are similar to those of Claim 32.

Therefore, it is rejected with the same rationale applied against Claim 32 above.

11. Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Lyle (U.S. Patent 6,886,012) as applied to claims 6-8 above, and further in view of Franczek et al. (U.S. Patent 6,397,335).

i. Referring to Claim 15:

As per Claim 15, Fink et al. and Lyle disclose a system in accordance with claim 6. Fink et al. and Lyle do not expressly disclose the remaining limitation of the claim. However, Franczek et al. disclose a buffer [i.e., a **Preferably, each virus-screening processor has an associated memory device to store at least two packets (lines 13-14, Col. 5)**] which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus [i.e., **Alternatively the virus screening can be performed in-line by partitioning the file into small blocks of data, screening each block of data, and communicating each virus-free block data upon being screened (lines 64-67, Col. 11)**]. Fink et al., Lyle, and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Lyle

with Franczek et al. to have a storage buffer for a large packet(s) to be inspected since one would be motivated to **examine one more succeeding blocks since a virus signature could extend over several blocks of data (lines 3-5, Col. 12 in Franczek et al.)**. Therefore, it would have been obvious to modify Fink et al. and Lyle with Franczek et al. to obtain the invention as specified in claim 15.

ii. Referring to Claim 16:

As per Claim 16, the rejection of Claim 7 is incorporated. In addition, Claim 16 encompasses limitations that are similar to those of Claim 15. Therefore, it is rejected with the same rationale applied against Claim 15 above.

iii. Referring to Claim 17:

As per Claim 17, the rejection of Claim 8 is incorporated. In addition, Claim 17 encompasses limitations that are similar to those of Claim 15. Therefore, it is rejected with the same rationale applied against Claim 15 above.

12. Claims 29-30, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Lyle (U.S. Patent 6,886,012), and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 15-16 above.

i. Referring to Claim 29:

As per Claim 29, the rejection of Claim 15 is incorporated. In addition, Claim 29 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 30:

As per Claim 30, the rejection of Claim 16 is incorporated. In addition, Claim 30 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iii. Referring to Claim 38:

As per Claim 38, the rejection of Claim 16 is incorporated. In addition, Claim 38 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

**(10) Response to Argument**

Applicant's arguments filed on Jun. 04, 2007 with respect to Claim Rejections under 35 U.S.C. 103(a) for Claims 1-55 have been fully considered, but they are not persuasive.

A. Claims 1, 3, 20-21, 32, 41-45, 47, 49-52, and 55 over Fink



1. Examiner disagrees with Appellant's argument that Fink fails to teach or suggest the claimed feature of virus scanning. Fink discloses the packet filter, which is composed of analysis module for analyzing packets and rule base containing rules which are defined for controlling the system **[Packet filter 22 in turn is preferably composed of an analysis module 24 for analyzing packets and a rule base 26. Rule base 26 preferably contains one or more rules which are defined according to the preferences of the system administrator or other controlling user. Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12 (lines 45-54, Col. 5)].** That is, the packet filter along with the analysis module and rule base functions as the claimed virus scanning engine, which receives the data packet, tests the data packet, and passes data packets to the destination if it meets the criteria (i.e., does not contain the virus/violation) and drop the packet if it does not meet criteria (i.e., contains the virus/violation). Fink further discloses the criteria of the rule base as determining whether packet represents a violation such as spoofing for anti-spoofing protection **[Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including**

information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 40-48, Col. 7). Such a message preferably includes a key for identifying the new connection, information concerning address translation and optionally information concerning encryption, both of which are processes which involve the modification of the packet itself. The key for identifying the new connection preferably includes such information as the source IP address and port, the destination IP address and port, the protocol field and optionally the interface(s) from which a packet is expected to be received, for anti-spoofing protection. The address translation information includes the translated source IP address and port, the destination IP address and port (lines 63-67, Col. 9 and lines 1-7, Col. 10)], and the packet may be dropped if it is not permitted [Also alternatively, under certain circumstances as described in greater detail below, the packet may be dropped, particularly with regard to packets received from firewall interface 42, which are optionally similarly analyzed. In order to avoid dropping packets which may not be IP packets, optionally and preferably, information regarding one or more "default" packet types may be stored in database 32, such that if such information is not stored in database 32, the packet is defined as being "not permitted" (lines 57-66, Col. 8)]. Therefore, the cited reference by Fink teaches the argued limitation about the virus scanning engine. Appellant may argue that spoofed packet may

not contain any virus and Examiner takes an overly broad view of virus scanning, and thus, Fink does not suggest any aspect of the claimed virus scanning. However, according to Appellant's definition of virus in the specification, the term, "virus", is not only limited to the malicious executable code, but rather any malicious data threat, and further not even limited to only "viruses" and "worms" (see parag. [0008] of the instant application). Therefore, the term "spoofing", which represents a violation as it contains forged information (i.e., malicious threat and/or a source of a spam or virus), in the prior art by Fink is sufficient to meet the claimed term of "virus", and any analysis of the packet in determining whether the packet is a spoofed one (i.e., containing forged information that caused any violation) satisfies the limitation regarding a packet containing a virus or not.

2. Examiner also disagrees with Appellant's argument that Fink fails to teach or suggest the claimed feature of classifying packets. Fink specifically teaches analyzing the data packet and determining if packet presents a violation (spoofing) or not **[Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12 (lines 51-54, Col. 5). Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determine that the packet represents a**

violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 40-48, Col. 7)]. That is, the data packet can either be a spoofed type (i.e., violation with malicious threat and/or a source of a spam or virus) or a non-spoofed type (i.e., no violation with malicious threat and/or a source of a spam or virus), and this fact is admitted by Appellant in the last line of page 7 of the Appeal Brief. Therefore, contrary to Appellant's argument, Fink teaches the claimed feature of classifying packets.

B. Claims 4-5, 11-14, 22-23, 27-28, 33, 36-37, 46, 48, and 53 over Fink in view of Franczek

Examiner disagrees with Appellant's argument that there is no teaching regarding the filtering of packets based on whether or not they can contain a virus. The prior art by Fink teaches the packet filter along with the analysis module and rule base functioning to perform the functions of receiving the data packet, testing the data packet, and passing data packets to the destination if it meets the criteria (i.e., does not contain the virus/violation) and drop the packet if it does not meet criteria (i.e., contains the virus/violation). Fink further discloses the criteria of the rule base as determining whether packet represents a violation such as spoofing for anti-spoofing protection **[Alternatively and optionally,**

even if only the interface is not correct, pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 40-48, Col. 7). Such a message preferably includes a key for identifying the new connection, information concerning address translation and optionally information concerning encryption, both of which are processes which involve the modification of the packet itself. The key for identifying the new connection preferably includes such information as the source IP address and port, the destination IP address and port, the protocol field and optionally the interface(s) from which a packet is expected to be received, for anti-spoofing protection. The address translation information includes the translated source IP address and port, the destination IP address and port (lines 63-67, Col. 9 and lines 1-7, Col. 10)]. The term "spoofing", which represents a violation as it contains forged information (i.e., malicious threat and/or a source of a spam or virus), in the prior art by Fink is sufficient to meet the claimed term of "virus". Therefore, the combination of Fink and Franczek is sufficient to meet Appellant's argument.

C. Claims 6-8, 24-25, 34, and 54 over Fink in view of Lyle

Examiner disagrees with Appellant's argument that as with Fink, Lyle fails to teach or suggest classifying received packets based on the type of packet. Once again, Fink specifically teaches analyzing the data packet and determining if packet presents a violation (spoofing) or not **[Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12 (lines 51-54, Col. 5). Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 40-48, Col. 7)].** That is, the data packet can either be a spoofed type (i.e., violation with malicious threat and/or a source of a spam or virus) or a non-spoofed type (i.e., no violation with malicious threat and/or a source of a spam or virus). Therefore, the combination of Fink and Lyle is sufficient to meet Appellant's argument.

D. Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 over Fink in view of Lyle and Franczek

Examiner disagrees with Appellant's argument that none of Fink, Lyle, and Franczek fails to teach or suggest filtering based on whether a packet can or cannot contain a virus. Once again, the prior art by Fink teaches the packet filter along with the analysis module and rule base functioning to perform the functions of receiving the data packet, testing the data packet, and passing data packets to the destination if it meets the criteria (i.e., does not contain the virus/violation) and drop the packet if it does not meet criteria (i.e., contains the virus/violation). Fink further discloses the criteria of the rule base as determining whether packet represents a violation such as spoofing for anti-spoofing protection **[Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 40-48, Col. 7). Such a message preferably includes a key for identifying the new connection, information concerning address translation and optionally information concerning encryption, both of which are processes which involve the modification of the packet itself. The key for identifying the new connection preferably includes such information as the source IP address and port, the destination IP address and port, the protocol field and optionally the interface(s) from which a**

**packet is expected to be received, for anti-spoofing protection. The address translation information includes the translated source IP address and port, the destination IP address and port (lines 63-67, Col. 9 and lines 1-7, Col. 10)].** The term “spoofing”, which represents a violation as it contains forged information (i.e., malicious threat and/or a source of a spam or virus), in the prior art by Fink is sufficient to meet the claimed term of “virus”. Therefore, the combination of Fink, Lyle, and Franczek is sufficient to meet Appellant’s argument regarding whether the or not the packet contains a virus.

E. Claim 40 over Fink in view of Radatti

Examiner disagrees with Appellant’s argument that as with Fink, Radatti fails to teach or suggest filtering packets based on whether or not the packets can or cannot contain viruses. Once again, the prior art by Fink teaches the packet filter along with the analysis module and rule base functioning to perform the functions of receiving the data packet, testing the data packet, and passing data packets to the destination if it meets the criteria (i.e., does not contain the virus/violation) and drop the packet if it does not meet criteria (i.e., contains the virus/violation). Fink further discloses the criteria of the rule base as determining whether packet represents a violation such as spoofing for anti-spoofing protection **[Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are**



other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 40-48, Col. 7). Such a message preferably includes a key for identifying the new connection, information concerning address translation and optionally information concerning encryption, both of which are processes which involve the modification of the packet itself. The key for identifying the new connection preferably includes such information as the source IP address and port, the destination IP address and port, the protocol field and optionally the interface(s) from which a packet is expected to be received, for anti-spoofing protection. The address translation information includes the translated source IP address and port, the destination IP address and port (lines 63-67, Col. 9 and lines 1-7, Col. 10)]. The term "spoofing", which represents a violation as it contains forged information (i.e., malicious threat and/or a source of a spam or virus), in the prior art by Fink is sufficient to meet the claimed term of "virus". Therefore, the combination of Fink and Radatti is sufficient to meet Appellant's argument regarding whether the or not the packet contains a virus.

#### **(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

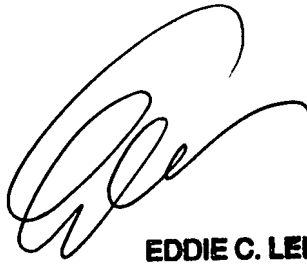
For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Yin-Chen Shaw/  
Shaw, Yin-Chen  
Aug. 30, 2007

Conferees:

Lee, Eddie C.



**EDDIE C. LEE**  
**SUPERVISORY PATENT EXAMINER**

Arani, Taghi T.

\Taghi T. Arani\

Supervisory Patent Examiner (Trainer)

Patent Training Academy